

Application Manager

Release Notes (Version 10.1)

These release notes include:

- [Components in this Release](#)
- [Important Upgrade Information](#)
- [New Features](#)
- [Bug Fixes](#)
- [Known Issues and Limitations](#)
- [Supported Operating Systems and Technologies](#)
- [Required Utilities and Components](#)

Components in this Release

Component	Version
Application Manager Agent	10.1.286.0
Application Manager Console	10.1.286.0
Analysis Server & Web Console	10.1.286.0

Important Upgrade Information

This upgrade section contains functionality changes that have been introduced in either Application Manager v10.0 or v10.1. Any information that is new to this release will be specifically listed as Application Manager v10.1.

We are including this extended information for the convenience of customers upgrading from an 8.x version.

Windows Client

Before attempting to install the v10.1 Agent the Microsoft Convenience Rollup KB2135574 should be applied to Windows 7 SP1. The Microsoft Security Monthly Quality Rollup KB3185330 should also be applied to Windows Server 2008R2.

Microsoft extended support for Windows XP ended on 8th April 2014, mainstream support for Windows Vista ended on 10th April 2012.

New Features

Windows Server 2016 Support

Application Manager 10.1 introduces a completely new driver, allowing a faster and more streamlined experience along with fewer reboots. This updated and improved driver supports Windows Server 2016.

Also:

- **Enhanced Windows Store App Support**
 - Further support has been added to the control of Windows Store Applications
 - Administrators may now block/allow all applications based on the 'Publisher' of the App, allowing control of Windows Store applications with fewer rules

- **Windows 10 OS Condition**
 - When creating a rule targeting Windows 10 devices, Application Manager now allows conditions using the Windows 10 build number (minimum, maximum, greater than, less than and equals)
 - Administrators may now block/allow applications, or elevate/restrict privileges, based on the Windows 10 build number.

Enhanced Ransomware Protection

Further protection for endpoints, as Application Manager 10.1 extends mitigation of ransomware:

- **PowerShell and JavaScript validation**
 - Specify which PowerShell and JavaScript scripts are allowed to run. Be more specific than ever before by only allowing trusted scripts and Java archives from trusted sources
 - Allow administrators to identify safe PowerShell scripts and Java archives without allowing users to introduce unknown ones
 - PowerShell and JavaScript files now adhere to 'Trusted Ownership' rules, meaning that scripts from untrusted sources cannot be launched

- **Process & Configuration Protection**
 - Prevent administrators from terminating the Application Manager process, or tampering with the Application Manager configuration to help ensure that users cannot circumvent protective measures
 - The "System Controls" feature of Application Manager has been extended to include the protection of *any* process, so that those specified processes are protected from termination by users including local administrators
 - For example, an Antivirus process, and can be protected from termination by all users, including admins.

- **Extended Metadata by checking Digital Certificate**
 - When verifying a file using metadata, administrators may now optionally compare the entire certificate to determine the authenticity of the file.
 - Checks can be made against the entire certificate for validity and that it hasn't been revoked.

Ease of Use

Enhancements have been made in several areas to simplify the configuration for Administrators, and provide more flexibility in creating a configuration policy for end users.

- **Extended Audit Logging**
 - New Events: Services Started/Stopped
 - Parent Process name now included in 9000 events
 - File Owner now included in 9000 events
 - The Determining Rule that applied the policy is now included in events
- **Self Elevation Enhancements**
 - Self Elevation has been extended to support all file types
 - Administrators may also specify that certain file extensions may only be elevated when open with certain applications (VBS with wscript.exe, for example)
- **Policy Change Request options moved to 'per-rule'**
 - Previously only set globally, administrators are now capable of enabling the Policy Change Request feature on a per-rule basis
 - This allows Policy Change Request to be enabled for some users, and not for others
 - Some settings remain global, such as the email address, telephone number and Shared Key.

Bugs Fixed

The following customer support issues have been resolved in this release.

Problem ID	Title	Details
13536	AAMP lockdown- implement protection for merging configs when secure AAMP feature is enabled	When the advanced setting: 'ConfigFileprotection' is enabled in a configuration and deployed to a client any configuration merging on this client should be blocked.
13525	Elevating Printer install which uses Web Services fails	With the "Printers" component configured for elevation in AM, a UAC prompt is still shown when trying to install a printer using the "Web Services" connection type.
11208	AM8.9 App Termination Spawns Multiple Message Boxes	AM Application Termination error box displays multiple times when using IP address for Computer Device rule.
13286	AM Config not being applied in non-persistent image at startup	AM configuration isn't being applied when Citrix MCS gold image boots. AM is installed without a configuration, the CCA installs the configuration at start-up.
13365	V10 Agents Fail to Install if KB31225574 installed instead of KB3033929	Trying to install any V10 agents when KB3125574 is installed fails with the error "Security Update for Windows (KB3033929) is already installed on this computer. This appears to be because KB3125574 is a roll up update that contains KB3033929.
13429	Comma replaced with space character in metadata from AM	Application Manager appears to be replacing commas with spaces in audited metadata. Citrix use a comma in their application metadata... GoToMeeting for example.
12097	Regedit.exe not blocked from Macro in office	When regedit.exe is set to be blocked in the AM configuration and it's launched from a macro in Office, it runs in spite of the configuration being in place.
12107	Event 9010 - incorrectly raised when using a PowerShell script	Run a PowerShell MA scripted rule that fails (does not meet condition) and you get event 9010 The scripted rule 'test success - dl-win7-2' failed to complete (Error: Source="*MACHINE*", Description="", Line="", Position='0') on '0'. The rule has not been applied.
12445	Redundant Registry Values are created during Installation	During the installation of AM 8.9 (Any version) it appears that the following value is created during installation: Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ Value: EcaEngine Data: EcaStandalone.exe
12574	Vidar Motion Application Crashing when managed by AM	Vidar Motion is crashing with Application Manager enabled
12575	Bloomberg Professional Installer crash with AM 8.8 SP1 / AM 8.9	When attempting to install Bloomberg Professional with Application Manager 8.8 SP1 or any version of 8.9 installed, the installation crashes with an Access Violation

Problem ID	Title	Details
12580	AM Console expands domain name incorrectly when computer name contains the domain name	When specifying a domain which contains the machine-name of the endpoint running the console, a variable is created with %computername% where the domain should appear
13049	PCR - 'Uninstall or Change a Program' behaves different to built-in elevate	Uninstallation of MSI's (installed via Windows Installer) not allowed by policy change request uninstall programs but is allowed by built-in elevate component for uninstall programs within URM in configuration.
13117	Self elevation in W10 tablet mode does not show virtual keyboard	When using self-elevation on a touch-screen device, when prompted for a reason for elevating an application, user cannot input a reason into dialogue box because virtual keyboard does not appear when trying to select this box.
13217	AM Blocking CSCRIPT but allows CSCRIPT.exe	AM blocks a VBScript when using only CS-script and not cscript.exe.
13219	Elevating built-in 'Disk Management' component causes CleanMgr.exe to crash	When launching the Disk Space Clean-up Manager utility (CleanMgr.exe) the process can crash if AM is being used to elevate the built-in 'Disk Management' component.
13455	Event ID 9023 logged incorrectly in AM v10	When 9023 (self elevate) events are raised on endpoint, the variables for reason given etc. are not expanded. The events also do not expand correctly in AMC.
11553	Self-Elevate (URM only) - Elevated MSI name does not appear in Local Event or AMC Logs	Auditing for self-elevation with MSIs does not show the full name of the MSI, on any AM 8.9 version including SP1 HF6 when the AAC feature is completely disabled in the configuration.
11572	Elevated websites render using IE7 engine	Elevated websites render using IE7 engine. Unable to using IE11 website features in AM 8.9 if the website is Elevated using AM
13467	Default Mail Client – Policy Change Request	There is an error that pops up when a user tries send in a policy change request. "Either there is no default mail client or the current mail client cannot fulfil the messaging request. Please run Microsoft Outlook and set it as the default mail client." Microsoft Outlook is the default mail client on the endpoint and when searching through the Default Programs menu, it is set as the default for all available options.
13279	Administrators can modify the AM config file	When logged on as an admin the user has the ability to modify the AAMP and OnDemand configurations allowing access to additional applications and processes
13041	Policy change request blank windows component drop down on Windows 10	Reported that in AM 8.9 SP3 HF1 there is an issue where when policy change request is in use, the drop down box for windows component will be blank.

Known Issues and Limitations

The known issues and limitations are now detailed on support.appsense.com.

Supported Operating Systems and Technologies

The supported Operating Systems and Technologies are now detailed in a compatibility matrix available on support.appsense.com.

Required Utilities and Components

Component	Required Utilities and Components
Console	Microsoft Windows Installer 5.0 Microsoft .NET Framework 4.6.x Microsoft Visual C++ 2015 Redistributable Package
Agent	Microsoft Windows Installer 5.0 Microsoft Visual C++ 2015 Redistributable Package
Web Service	Microsoft Windows Installer 5.0 Microsoft Visual C++ 2015 Redistributable Package Microsoft .NET Framework 4.6.x



Note

Please ensure that your endpoints are fully up to date with the latest patches from Microsoft.